PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 19/00, H04L 9/32, G07F 7/08	**A1**	**(11) International Publication Number:** **WO 99/26207** **(43) International Publication Date:** 27 May 1999 (27.05.99)

(21) International Application Number: PCT/US98/24597

(22) International Filing Date: 18 November 1998 (18.11.98)

(30) Priority Data:
60/066,137　　　19 November 1997 (19.11.97)　US

(71) Applicant: SECURITY DYNAMICS TECHNOLOGIES, INC. [US/US]; 20 Crosby Drive, Bedford, MA 01730 (US).

(72) Inventor: JUELS, Ari; Apartment 205, 4 University Road, Cambridge, MA 02139 (US).

(74) Agent: HEFFAN, Ira; Testa, Hurwitz & Thibeault, LLP, High Street Tower, 125 High Street, Boston, MA 02110 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DIGITAL COIN TRACING USING TRUSTEE TOKENS

(57) Abstract

A system and method for obtaining traceable anonymous digital cash from a bank using a trustee as a trusted third–party. A user establishes his identity with the trustee using a secret known by the user. The user transmits to the trustee information describing a blinded traceable digital coin. The user receives from the trustee a trustee token including a signature by the trustee on the blinded coin. The user transmits the blinded coin and the trustee token to a bank. The user receives a signature from the bank certifying the blinded coin. The user can then unblind the coin, and spend the coin at a merchant. The system and method support both tracing of the identity of a user from a coin, referred to as coin tracing, and generation of a list of all coins belonging to a given user, referred to as owner tracing. Both of these operations require very little computation and database access. To determine the identity of the user, the trustee can generate the list of coins associated with a user. Alternatively, if presented with a coin, the trustee can determine the identity of the user who submitted the coin to the trustee for signature. This simple and highly efficient trustee–based tracing system and method can be added on top of anonymous cash schemes based on blind RSA signatures.

DIGITAL COIN TRACING USING TRUSTEE TOKENS

Cross-Reference to Related Application

This application claims priority to U.S. provisional patent application serial number 60/066,137 filed November 19, 1997.

Technical Field

5   This invention relates to the field of electronic commerce transaction systems and, more particularly, to the tracing of anonymous digital cash.

Background Information

Digital cash, also known informally as e-cash, is a form of digital currency. Cash is represented by electronic (digital) coins. As with ordinary coins, each digital coin has a fixed

10   denomination. Coins are "issued" by a coin issuer, also referred to as a bank. Using cryptography, a bank signs a coin to certify the coin's authenticity.

In some electronic cash systems, such as the ECASH system commercially available from DIGICASH of Palo Alto, California, a user authenticates herself in a secure manner to a bank. The user then withdraws coins, which are numbers (or sets of numbers) that represent money,

15   from the bank. The bank deducts funds corresponding to the withdrawn coins from her account. To spend a coin with a merchant, the user simply transmits the coin to the merchant. To prevent double spending of a coin, the merchant verifies on-line with the bank that the coin has not already been spent. An explanation of the DIGICASH protocols can be found in B. Schoenmakers, "Basic Security of the ecash™ Payment System," which appears in Computer

20   Security and Industrial Cryptography: State of the Art and Evolution, ESAT Course 1997, edited by Bart Preenel et al.

One type of cryptography used in electronic cash systems is public/private key cryptography. One commercially available public/private key technology is RSA encryption technology, available from RSA Data Security, Inc. of San Mateo, California. To provide a

25   simplified overview, an RSA signature is based on the difficulty of computing roots, for example cube roots, modulo a large modulus N with unknown factorization. A signer knows the factorization of the modulus N and so the signer is the only entity able to compute $f^{1/n}(x)$ mod N,

- 2 -

for a given (x), where f is a one-way collision-free hash function, and $f^{1/n}(x)$ mod N represents the nth root of f(x) modulo (N). In the implementation of digital cash, a user who presents a merchant with the valid pair $(x, f^{1/n}(x)$ mod N), where n and N are publicly known numbers chosen by the bank, effectively demonstrates that the coin (x) has been authorized (or signed) by the bank,

5   because only the bank can determine $(f^{1/n}(x)$ mod N) from x. To distinguish among different denominations in this scheme, the bank can use different public exponents. For example, $(x, f^{1/3}(x)$ mod N) might indicate a \$0.50 coin, while $(x, f^{1/17}(x)$ mod N) might indicate a \$1 coin.

Digital coins have been implemented that are both secure (in the bank's interest) and afford a heightened assurance of consumer privacy by providing anonymity to users with respect

10   to both merchants and banks. Informally, a digital cash scheme is referred to as unconditionally blind or anonymous if the bank that issues a coin is unable to determine, either at the time of withdrawal or later upon examining circulating or deposited coins, which coin was withdrawn by which user. The user can withdraw money from the bank in such a scheme, spend it at a merchant, and be confident that when the merchant deposits the money at the bank, the bank will

15   not be able to recognize the money as the same cash given to the user.

There are several variants of anonymous digital cash, not all of which have been implemented commercially. In a commercially available, on-line version implemented by DIGICASH, a coin consists of an RSA signature by the bank on the hash of a message (x). In this blinded protocol, the bank signs coin (x) by calculating $(f^{1/n}(x)$ mod N) without knowing what

20   (x) is. At the time the coin is submitted to the bank for signature, the coin (x) is "hidden" from the bank by a blinding factor, which the user "multiplies in" and combines with (x) before transmission to the bank and "divides out" after the bank has signed.

Referring to FIG. 1, the bank publishes a public modulus N=pq, for which it alone knows the factorization (pq), and chooses a public exponent, which for this example is the exponent 3

25   (i.e. cube root). A user chooses random numbers (x) and (r), where (x) is the number to be used in the coin, and (r) is a blinding factor and $(x) \in_r Z_N$ and $(r) \in_r Z_N$, meaning that (x) and ® are integers between (0) and (N-1) inclusive. The user calculates f(x) mod N, and multiplies the result by the blinding factor (r^3). The user sends $(r^3 f(x)$ mod N) to the bank. The bank determines the cube root mod N, which only the bank can do because the bank knows the factors

30   (pq) of (N). The bank never knows (x), however, because it receives f(x) multiplied by the blinding factor (r^3). The bank then returns $(r\, f^{1/3}(x)$ mod N) to the user. The user extracts $f^{1/3}(x)$

- 3 -

from the quantity (r $f^{1/3}(x)$ mod N) it receives from the bank by dividing by (r). The user then can provide a merchant with the "signed" coin (x, $f^{1/3}(x)$). The merchant can verify that the bank has signed the coin (x, $f^{1/3}(x)$) by calculating f(x) mod N from x, and comparing it to the cube of ($f^{1/3}(x)$) modulo (N). This protocol is unconditionally blind, because the blindness does not rely on computational assumptions or statistical arguments.

A weaker notion of blindness can be described informally in terms of a lack of statistical correlation between the view of the signer at the time of signing and the set of produced signatures. A more formal definition of computational blindness may be described in terms of the following experiment. The user produces two messages m_0 and m_1 of length polynomial in k_1. The user sets a bit (b) uniformly at random. In two arbitrarily interleaved (and presumed blind) digital signature protocols, she presents the documents m_0 and m_1 to the bank in an order specified by (b), i.e., in the order $\{m_b, m_{1-b}\}$. In this interaction, she obtains from the bank signatures $s(m_0)$ and $s(m_1)$ on the two messages. The user presents the message/signature pairs (m_0, $s(m_0)$) and (m_1, $s(m_1)$) to the bank. The bank then attempts to guess the bit b. If no polynomial-time algorithm exists which enables the bank do so with probability $1/2 + 1/poly$ (over its own coin-flips and those of the user), then we say that the digital signature scheme is blind or secure with respect to anonymity.

Researchers have observed that unconditional anonymity in payment systems might be exploited to facilitate crimes like blackmail and money laundering. This observation spurred research into the idea of making anonymity in payment systems conditional, and, in particular, revocable by a third party. This notion is referred to as a trustee-based coin tracing. A National Security Agency report has since declared the availability of tracing in e-cash systems vital to the security interests of the United States. The importance of traceability in e-cash systems has motivated the proposal of various trustee-based coin tracing schemes.

One trustee-based tracing scheme is based on a blind Schnorr-like signature scheme and involves use of interactive proofs between trustees and the bank. Another trustee-based tracing scheme is based on blind RSA signatures, but make use of a cut-and-choose protocol, resulting in a scheme that is flexible but has rather large coin sizes and computational requirements.

Another scheme makes use of a blind signature based on that of Chaum and Pedersen. In this scheme, the user requests a pseudonym and registration information from a trustee. The user

- 4 -

presents this registration information to the bank, and also incorporates it into the coins she withdraws.

Another scheme introduces the notion of "challenge semantics," enabling flexible determination of coin value, so that coins can be invalidated, for example in case of a bank
5   robbery. This scheme is capable of addressing stronger attack models than many others and a wider range of commercial settings. It is also adaptable to use with any underlying digital signature scheme. On the other hand, this scheme requires on-line participation of a trustee in both coin withdrawal and coin spending.

Another scheme, referred to as "Magic Ink," makes use of blind DSS signatures. In this
10   scheme, signing and anonymity revocation can be conducted by differing quorums of trustees. trustees are again, however, fully on-line, and the scheme is also rather computationally intensive for most operations.

A slightly different approach to trustee-based tracing is a system based on blind Schnorr signatures in which a user transfers funds from a non-anonymous to an anonymous account, and a
15   trustee is capable of linking the two accounts. The chief disadvantage of this approach is that once the two accounts are linked, anonymity is eliminated.

Another approach is based on blind Schnorr signatures in which the trustee is wholly off-line. This system is quite complex, and involves well over a dozen modular exponentiations by the user at each coin withdrawal. Later developments reduced the computation required in the
20   withdrawal protocol, as well as the database search requirements in owner tracing. The withdrawal protocol, however, still requires over a dozen modular exponentiations on the part of the user.

In addition to the above-described inefficiencies, the schemes described above involve changes or additions to the underlying structure of the coins. The therefore cannot be readily
25   adapted to existing digital cash systems.

Summary of the Invention

A simple and highly efficient trustee-based tracing mechanism is provided that can be added on top of anonymous cash schemes based on blind RSA signatures. The scheme can support both tracing of the identity of a user from a coin, referred to as coin tracing, and

- 5 -

generation of a list of all coins belonging to a given user, referred to as owner tracing. Both of these operations require very little computation and database access.

The tracing mechanism according to the present invention has several important advantages over prior schemes. It can be incorporated straightforwardly on top of a
5 commercially implemented on-line anonymous e-cash scheme, for example DIGICASH, with no change to the structure of the coins or the spending or deposit protocols, and can be easily applied to off-line e-cash variants as well. The tracing mechanism according to the present invention imposes minimal computational overhead on the underlying withdrawal scheme for the user -- essentially just several modular multiplications and a Message Authentication Code
10 ("MAC"). Most other schemes carry overhead for the user amounting to several modular exponentiations per transaction, which means as much as one hundred times more computation. Computational and storage requirements for the bank are also minimal. The tracing operation is also highly efficient. In the case of coin tracing, for instance, this scheme requires no database lookups, which most other schemes do. The tracing mechanism according to the present
15 invention is also provably secure with respect to underlying cryptographic primitives.

The tracing mechanism requires user registration with a trustee upon set up of the user's account (and possibly again later, if the user spends a large number of coins). As a result of this interaction between user and trustee, the system requires storage of a small amount of authorization data for withdrawals. It should also be noted that to incorporate multiple trustees
20 the system uses what amounts to a trusted dealer.

In general, in one aspect, the invention features a method for obtaining a trustee token from a trustee. The method includes transmitting to a trustee information describing a blinded digital coin and receiving from the trustee a trustee token comprising a signature by the trustee on the blinded coin.

25 Embodiments of this aspect of the invention include the following features. In one embodiment, the information describing the blinded digital coin is the blinded digital coin. In another embodiment, the information describing the blinded digital coin comprises a random seed for generating one or more blinded digital coins. In another embodiment, the information describing the blinded digital coin further comprises a quantity of desired coins for generating the
30 quantity of desired blinded digital coins. In another embodiment, before the transmitting step, the

- 6 -

method includes establishing identity with the trustee using a secret. In another embodiment, the secret comprises a public/private key pair.

In general, in another aspect, the invention features a system for obtaining a trustee token from a trustee. The system includes a transmitter transmitting to a trustee information describing

5   a blinded digital coin, and a receiver receiving from the trustee a trustee token comprising a signature by the trustee on the blinded coin. In one embodiment, the trustee token comprises a signature by the trustee on one or a plurality of blinded coins.

In general, in another aspect, the invention features a method for generating a trustee token. The method includes receiving from a verified user information describing a blinded digital

10   coin. Information describing the blinded digital coin and a verified user identifier are stored. A trustee token comprising a signature by a trustee on the blinded coin is generated using the information describing the blinded digital coin.

Embodiments of this aspect of the invention include the following features. In one embodiment, the the information describing the blinded digital coin is the blinded digital coin. In

15   another embodiment, the information describing the blinded digital coin comprises a random seed for generating one or more blinded digital coins. In another embodiment, the information describing the blinded digital coin further comprises a number of desired coins for generating one or more blinded digital coins. In another embodiment, the trustee token includes the trustee's signature on one or a plurality of coins. In another embodiment, after the generating step, the

20   trustee token is transmitted to the user. In another embodiment, before the receiving step, the identity of the user is verified using a secret. In another embodiment, the generating step includes generating a trustee token by using the information describing the blinded digital coin to generate the blinded digital coin, and signing the blinded digital coin. In another embodiment, the blinded digital coin is signed using a private key of a public/private key pair. In another embodiment, the

25   blinded digital coin is signed using a Message Authentication Code ("MAC").

In general, in another aspect, the invention features a system for generating a trustee token. The system includes a receiver for receiving from a verified user information describing a blinded digital coin, a data store for storing the information describing the blinded digital coin and for storing a verified user identifier, and a token generator for generating a trustee token using the

30   information describing the blinded digital coin. In one embodiment, the trustee token is a signature by a trustee on the blinded coin.

- 7 -

In general, in another aspect, the invention features a method for issuing digital cash. The method includes receiving a blinded coin and a trustee token from a verified user. In one embodiment, the trustee token is a signature by a trustee on a blinded coin. The method also includes verifying the trustee token, deducting an amount from an account associated with the user, and issuing the blinded coin with a value related to the amount deducted from the user's account.

Embodiments of this aspect of the invention include the following features. In one embodiment, before the receiving step, the identity of the user is verified using a secret. In another embodiment, the verifying step comprises calculating a Message Authentication Code ("MAC") on the blinded coin. In another embodiment, the verifying step includes verifying a trustee's public key. In another embodiment, the issuing step comprises signing the blinded coin.

In general, in another aspect, the invention features a system for issuing digital cash. The system includes a receiver for receiving a blinded coin and a trustee token from a verified user. The trustee token includes a signature by a trustee on a blinded coin. The system also includes a verifier for verifying the trustee token, a withdrawl mechanism for deducting an amount from an account associated with the user, and an issuer for issuing the blinded coin with a value related to the amount deducted from the user's account.

In general, in another aspect, the invention features a method for receiving digital cash from a coin issuer using a trustee token. The method includes transmitting a blinded digital coin and a trustee token to a coin issuer. The trustee token includes a signature by a trustee on the blinded coin. The method also includes receiving a signature on the blinded digital coin from the coin issuer.

In general, in another aspect, the invention features a system for receiving digital cash from a coin issuer using a trustee token. The system includes a transmitter transmitting a blinded digital coin and a trustee token to a coin issuer. The trustee token includes a signature by a trustee on the blinded coin. The system further includes a receiver receiving a signature on the blinded digital coin from the coin issuer.

In general, in another aspect, the invention features a method for obtaining revokably anonymous digital cash from a bank by using a trustee. The method includes establishing identity with the trustee using a secret, transmitting to the trustee information describing a blinded digital coin, receiving from the trustee a trustee token comprising a signature by the trustee on the

- 8 -

blinded coin, transmitting the blinded coin and the trustee token to a bank, and receiving a signature from the bank certifying the blinded coin. Embodiments of this aspect of the invention further include unblinding the coin and transmitting the coin to a merchant.

In general, in another aspect, the invention features a method for tracing a digital coin. The method includes decrypting the coin to reveal a user identifier and matching the user identifier encrypted in the coin to an entity.

In general, in another aspect, the invention features a method for identifying a digital coin associated with a user. The method includes matching the user to a user identifier, matching the user identifier to coins transmitted to a trustee, and identifying the coins matched to the user identifier as coins associated with the user.

In general, in another aspect, the invention features a trustee token comprising a signature by a trustee on a blinded coin. In one embodiment, the trustee token comprises a signature by a trustee on one or more blinded coins. In another embodiment, the trustee token comprises a signature by a trustee on a plurality of blinded coins.

The foregoing and other objects, aspects, features, and advantages of the invention will become more apparent from the following description and from the claims.

Brief Description of the Drawings

In the drawings, like reference characters generally refer to the same parts throughout the different views. Also, the drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention.

FIG. 1 is a prior art anonymous digital cash scheme;

FIG. 2 is an embodiment of a traceable anonymous digital cash system according to the present invention;

FIG. 3 is a block diagram depicting an embodiment of the trustee token withdrawal protocol according to the present invention;

FIG. 4 is a block diagram depicting another embodiment of trustee token withdrawal protocol according to the present invention; and

FIG. 5 is a block diagram depicting an embodiment of the coin issuer withdrawal protocol according to the present invention.

- 9 -

Description

Referring to FIG. 2, an anonymous digital cash scheme according to the present invention can include a bank (B) 14, a trustee (T) 16, a user (U) 10, and a merchant (M) 12. In one embodiment, the bank 14, trustee 16, user 10, and merchant 12 functionality described below are implemented with software running on commercially available general purpose computers, including for example a personal computer or a smartcard. In other embodiments, any of the bank 14, trustee 16, user 10, and merchant 12 functionality can be implemented as special-purpose hardware. Any of the bank 14, trustee 16, user 10, and merchant 12 can be in the same physical location or in different locations, providing there is a communications channel or channels between them, such as a data bus, network, or link that allows them to communicate as described below. Such a communications channel can always be active, as can be achieved by dedicated link to a data network, or may be periodically connected, such as with a dial-up data connection, or by connecting a smartcard to a reader, or by use of a store-and-forward communcations link.

The bank 14 is a coin issuer, which can be a financial institution that issues anonymous digital coins and manages accounts. The user 10 withdraws digital cash from the bank 14 in the form of coins, which are numbers that are signed by the bank 14. The coins can be spent at a merchant 12. In one embodiment, the bank 14 publishes an RSA modulus (N), where $(N=pq)$, whose factorization (pq) the bank 14 alone knows.

The trustee 16 is a trustworthy (i.e. secure and reliable) device or agency responsible for tracing coins. In one embodiment, the trustee 16 holds a secret key (SK_T) for some public key encryption algorithm and the trustee publishes the corresponding public key (PK_T). In one embodiment, the trustee 16 also holds a symmetric key (w), which it shares with the bank 14.

In one embodiment, the trustee is responsible for tracing coins upon presentation of a court order by a government or other authorized agency. In one embodiment, the trustee 16 acts as a neutral third-party in the transaction between the user 10 and the bank 14. The trustee 16 has information mapping a user's identity to digital coins. In one embodiment, to communicate with the trustee 16, the user 10 possesses a unique identifier or account number denoted by ID_U, and also a secret s_U associated with ID_U and used to prove the user's identity. The secret s_U can be a public/private key, symmetric key, or other type of authentication, such as a password or

- 10 -

biometric characteristic. The trustee 16 can match the user identifier ID_U to the user's real-world identity.

In one embodiment, the bank 14 also recognizes the user identifier ID_U. In another embodiment, the user 10 is identified to the bank 14 by an alternate identifier ID_U' that is different

5   from the identifier ID_U that identifies the user 10 to the trustee. Alternatively, the bank can transact with the user on an entirely anonymous basis using only account information.

The merchant 12 is any party with whom the user spends money. Anonymous digital cash tracing according to the present invention does not require modification of the underlying digital cash protocols involving the merchant, i.e., the spending and deposit protocols, and so these

10 protocols are not discussed in detail. In one embodiment, the coin is chosen so that the value used for the coin can be identified with a particular user by the trustee and so there is no need for any change to the coin or to the spending and deposit protocols.

In the following discussion, (f) denotes a secure one-way or hash function, and $MAC_w(m)$ denotes a Message Authentication Code ("MAC") computed using symmetric key (w). Message

15 Authentication Codes, also referred to as key-dependent one-way hash functions, are described in the Handbook of Applied Cryptography by A.J. Menezes, PC. van Oorschot, and S.A. Vanstone, CRC Press 1996. $E_{PK_X}(m)$ denotes the encryption (under some appropriate asymmetric cipher) of the message (m) using the public key PK_X. The notation (PS) denotes an indexed pseudo-random generator, although other generators, for example a chained generator, can be used as well. The

20 notation $PS_A(i)$ denotes the output of the generator with secret seed (A) on index (i). The set $\{X_i\}$ denotes the set of values X_i over all appropriate values of i. The symbol $\|$ denotes concatenation of strings, $\oplus$ denotes the XOR operation, and $\in_R$ denotes uniform random selection from a set.

Three security parameters are denoted by k_1, k_2, and k_3. The parameter k_1 is the length of

25 the seed to the pseudo-random number generator (PS), and thus specifies the level of security on the user's anonymity. The parameter k_2 specifies the length of the digital signature modulus (N) used by the bank for signing coins, and thus the hardness of existential forgery. The parameter (k_3) specifies the length of the trustee tokens or MACs. This is essentially equivalent to the level of security on the trustee's ability to trace the user's coins. The notation $1/2 + 1/poly$ denotes a

- 11 -

probability greater than or equal to $1/2 + 1/k^c$, where (c) is some constant and (k) is the pertinent security parameter.

Referring again to FIG. 2, in one embodiment, before interacting with the bank, the user 10 sends one or more blinded coins C_i 22, or information sufficient to generate one or more blinded coins C_i 22, to the trustee 16. In response, the user 10 obtains from the trustee 16 one or more corresponding trustee tokens M_i 24. The trustee tokens M_i 24 are essentially proof that the blinded information the user is presents to the bank has been seen and its correctness verified by the trustee. In one embodiment, the trustee tokens M_i 24 are 10-50 bits, which are short enough to be useful and long enough to assure security, although it should be clear that the number of the bits in the trustee token M_i is not a limitation on the invention. A trustee token M_i is presented to the bank when the user withdraws money. A trustee token M_i reveals no information to the bank about the coin the user obtains. For the sake of simplicity, in the following discussion, one trustee token M_i is described for each coin withdrawal. As described later, a single trustee token M_i can be used for multiple coins.

To obtain trustee tokens, the user 10 contacts a trustee 16. The user 10 establishes the user's identity ID_U with the trustee 16, for example using secret s_U. Once the user's identity has been established with the trustee 16, the user 10 sends blinded coins to the trustee 16. Alternatively, as in the embodiment of FIG. 4 described below, the user 10 can send information describing the coins, and the trustee 16 generates the blinded coins. The trustee 16 can match the coins to the user's identifier ID_U, even after the coins have been unblinded. The blinded coins are signed by the trustee 16. The trustee's signature of the coins C_i comprises the trustee token M_i. In one embodiment, the signature is a digital signature using public/private (asymmetric) key encryption. In another embodiment, the signature is a MAC that is determined using symmetric encryption. The signature can made using encryption with a asymmetric or a symmetric key.

By requesting many trustee tokens in advance of coin withdrawals, and batching trustee tokens so that they apply to multiple coins (as described later), the user can achieve a very low frequency of interaction with the trustee 16. For example, user-trustee interaction can be limited to account set-up, or to account set-up and infrequent, off-line communications.

In some anonymous digital cash withdrawal protocols such as the DIGICASH protocol described above, to obtain a coin $(x_i, f^{1/n}(x_i) \bmod N)$ the user sends to the bank the blinded

quantity $r_i^n f(x_i)$ mod N. If the quantity (x_i) contains information sufficient to identify the user 10 to the trustee 16, then it is possible to have coin be revocably anonymous without a change to the structure of the coin.

In one embodiment, the user's identifier ID_U is concatenated with a pseudorandom value and encrypted under the public key of the trustee, so that $(x_i = E_{PKT}(ID_U \| s_i)$, where $s_i = PS_S(i))$. The quantity (x_i) thus can be computed from seed (S) and identifier (ID_U). The blinding integer (r_i) is generated from a random seed (R), so that $r_i = PS_R(i)$. These coins can be generated by the user and sent to the trustee for verification and signature.

Alternatively, if the trustee has an identical pseudorandom generator, just the seed need be sent to the trustee, and the trustee can generate the coins. In one embodiment, the user transmits random seeds (R) and (S) to the trustee, and the trustee generates the desired trustee tokens. The seeds (R) and (S) constitute all of the data required by the trustee to perform owner tracing against the user. Note that (R) and (S) are given as separate seeds for notational convenience. In practice, they may be combined into a single seed. The transmission of only the random seed provides communication and storage efficiency.

In the following discussion of the trustee token and coin withdrawal protocols, the computations are performed (mod N). To simplify notation, explicit indication of the (mod N) calculation may be omitted.

Referring to FIG. 3, in STEP 110 and STEP 114, the user proves her identity to the trustee. This can be accomplished using a secret S_U 112, which may be a public/private key, symmetric key, or other type of authentication, such as a password or biometric characteristic. In STEP 116, the user chooses a seed that is used to generate one or more coins (C_i) 120. In the embodiment of FIG. 3, the seed is has elements (R),(S). In STEP 118, for each coin (C_i) 120 the user determines $s_i = PS_S(i)$, and then determines $x_i = E_{PKT}(ID_U \| s_i)$. If there are j coins (C_i), the user will determine x_i for each i from 1 to j. Having determined x_i, the user determines $r_i^3 f(x_i)$, which is the blinded coin. The user transmits the coin (C_i) to the trustee. The trustee stores the user's identifier ID_U along with the coin (C_i). The trustee can verify that it can extract the user identifier ID_U from the coin, that is the trustee can verify that the coin is well formed. In STEP 126, the trustee calculates a MAC on the blinded coin $(r_i^3 f(x_i))$ using (w), the symmetric key that the trustee shares with the bank, STEP 126. The trustee's signature of the coin(s) (C_i) comprises

the trustee token. The trustee sends the trustee token back to the user in step 128. To prevent compromise of the coin and the trustee tokens, communication between the user and the trustee can take place over an authenticated and encrypted channel.

In other embodiments, it is possible for the user to send, instead of the coin 120, information which makes it possible for the trustee to generate the coin 120. In one such embodiment, and referring to FIG. 4, STEP 110, 114, 116, and 118 are the same, but instead of the user transmitting the coin to the trustee, the user transmits the seed (R),(S) and the desired number of coins j 130. In STEP 132, the trustee stores the user identifier ID_U and the seed (R),(S). In STEP 134, the trustee generates one or more coins C_i from the user identifier ID_U, and the seed. The trustee then generates a trustee token for the coin(s) C_i by calculating a MAC on the blinded coin $(r_i^3 f(x_i))$ using (w), the symmetric key that the trustee shares with the bank, STEP 136. The trustee's signature of the coin(s) (C_i) comprises the trustee token. The trustee sends the trustee token back to the user in step 128.

The user can request and store a large number of trustee tokens, since tokens are small. These tokens may be used for future withdrawals without the need for additional contact with the trustee until the user exhausts her supply. The tokens can be stored with the coins, or to save space a MAC for a quantity of coins can be stored with the seed/quantity information so that the coins can be regenerated later.

Although the token withdrawal protocol is described as an interaction with an on-line trustee, it will be understood that this is not a limitation. For example, trustee tokens can be requested using a secure store-and-forward system, or, alternatively, loaded on a smart card by the trustee.

Referring to FIG. 5, one embodiment of the coin withdrawal protocol is essentially the same as in the underlying electronic cash protocol, with the exception that the bank verifies, by means of a valid trustee token, that the user's withdrawal request has been authorized by the trustee. The user establishes identity with the bank STEP 150, STEP 152. This can be accomplished using a secret S_U' 154, which may be a public/private key, symmetric key, or other type of authentication, such as a password or biometric characteristic. The secret S_U' that the user shares with the bank may be the same or different from the secret S_U that the user shares with the trustee. Having authenticated itself to the bank, the user can transmit to the bank one or more

- 14 -

blinded coins. If the user has not stored the blinded coins, then the user generates $(r_i^n f(x_i))$ from (x_i, r_i), where (x_i, r_i) is generated from $(R), (S)$ by determining $s_i = PS_S(i)$, $x_i = E_{PKT}(ID_U \| s_i)$, and $r_i = PS_R(i)$. If the user has stored the coin(s), it is not necessary to regenerate the coin(s), and in STEP 158 the user transmits to the bank the coin(s) along with the trustee token $(r_i^n f(x_i)), M_i)$ 160 received from the trustee. The bank verifies $M_i = MAC_w(r_i^n f(x_i))$ using the symmetric key w that it shares with the bank (STEP 162). If the MAC is correctly formed, meaning that the trustee has certified that it is storing the appropriate tracing information, then in STEP 164 the bank determines the root $(r_i f^{1/n}(x_i))$ and transmits the result 166 back to the user. The user can then unblind the coin and verify the correctness of the coin, by calculating $f(x_i)$, and by multiplying $f^{1/n}(x_i)$ by itself n times, and comparing the two results (STEP 168). To prevent theft of the user's coins, the coin withdrawal protocol can take place over an authenticated and encrypted channel (on which even the trustee cannot eavesdrop).

In one embodiment, the trustee tokens are used with off-line variants of Chaumian e-cash (such as the Untraceable Electronic Cash described by Chaum, Fiat, and Naor in Advances in Cryptology - CRYPTO '88). Off-line ecash variants involve the user's embedding tracing information in coins that gets revealed when a coin is double-spent. To employ trustee tokens, then, in an off-line scheme, it suffices for the user to generate this tracing information from the seed (S). The tracing scheme of the present invention can make off-line systems more efficient by allowing the trustee to verify coin information incorporated to prevent double-spending.

To trace a coin C_i, the trustee is given the coin (x_i). Since $x_i = E_{PKT}(ID_U \| s_i)$, the trustee may extract ID_U from a coin C_i simply by performing a decryption with its secret key SK_T. The user identifier ID_U will then be revealed.

To perform owner tracing, the trustee is given a user identifier ID_U. In one embodiment, the trustee can look up all the coins (C_i) associated with the user identifier. In another embodiment, the trustee has stored $(R), (S)$, with the associated user identifier. The trustee uses (S) to compute all $\{x_i\}$. This is sufficient to identify all coins withdrawn by the user ID_U.

If the trustee is presented with a single coin, the trustee can extract the user identifier ID_U from the coin, and then determine all other coins associated with that user identifier ID_U. In contrast to some other schemes, it is possible for the trustee to identify not only all coins

- 15 -

withdrawn by the user and subsequently deposited, but also all coins in current circulation, and even some coins to be withdrawn by the user in future transactions.

As explained above, the trustee-based tracing scheme adds very little computational overhead to the underlying coin withdrawal protocol. The bank computes a MAC that it would not otherwise compute, but this requires negligible effort in comparison with generation of the signature on the coin. The user must compute the values (r_i) and (x_i) from a pseudo-random generator, but these values would likely be computed in some pseudo-random fashion in any case. In fact, if the bank uses a signature exponent of 3, the user need only compute two pseudo-random values, a hash, six modular multiplication operations, and a modular inversion per withdrawal (including verification that it has a valid coin). This is an improvement over some schemes that, for example, require fifteen (160 bit) modular exponentiation operations on the part of the user at the time of withdrawal, and even more if the scheme is to permit owner tracing.

The token withdrawal process requires no computationally intensive cryptographic operations - just a few hashes and computations of MACs. The storage requirements for trustee tokens are also minimal. The trustee stores a pseudo-random seed for each user (perhaps 80 bits). In the scheme described above, the user stores a minimal amount, for example 10-100 bits, for each trustee token. A coin in some other schemes consists of roughly 1000 bits. Hence, the storage of a collection of trustee tokens will not be difficult on a device capable of storing anonymous digital cash. In fact, at 10 bits per token, 1K bytes of memory is enough to store more than 800 trustee tokens.

For the sake of simplicity, we have assumed in the above description of our scheme that one trustee token is used for every withdrawal. It is possible to improve the storage efficiency of trustee tokens substantially by making a single trustee token good for multiple withdrawals., at the cost of some linkage of user identity across coin. Suppose, for instance, that the user always withdraws coins in multiples of ten. Then we could let $M_j = MAC_w(r^3_{10j}f(x_{10j}), r^3_{10j+1}f(x_{10j+1}), \ldots, r^3_{10j+9}f(x_{10j+9}))$. In other words, the MAC is calculated on ten coins. A first token M_0 is good for the first ten withdrawals, M_1 for the next ten withdrawals, etc. In fact, it is not even necessary for the user to withdraw coins in groups of ten. With a very slightly more complicated protocol, the user can send all ten coins for calculation of the MAC, but only request a withdrawal of a subset of the coins. In other words, the user need only send a number of blank withdrawal requests, i.e., a sequence of $r_i^3 f(x_i)$ for which she does not wish to receive the corresponding coins. Note that if

- 16 -

one token is to be used for multiple withdrawals, then it is probably desirable for the token to be
larger than it would be for one withdrawal. A token of length, say, 50 bits, should be adequate for
most any application. If enough batching is performed, it may be efficient to use digital signatures
instead of MACs, eliminating the need for secret key establishment between the trustee and bank.
5   Of course, making a single trustee token good for multiple withdrawals comes at the cost of some
linkage of user identity across coins.

One embodiment of a system according to the present invention is optimized for use with
cash carrying devices containing relatively small amounts of memory and for trustees with limited
database resources. Of course, trustee tokens may be used to achieve a wide range of tradeoffs
10   involving protocol efficiency, storage requirements, security levels, and token sizes. It may also
be helpful to store trustee tokens in different data structures, such as hash trees.

The system has been described as having only a single trustee. It is possible to achieve k-
out-of-n tracing with any number (n) of trustees by sharing the secret SK_T among the (n) trustees
in an initialization phase. It is also necessary, however, to share (R), (S), and ID_U for each user
15   after the corresponding trustee tokens have been distributed. Sharing may be performed using any
of a number of threshold and/or proactive secret-sharing techniques.

While flexible, this method of incorporating multiple trustees into our scheme achieves
weaker security guarantees than some other systems. The secrets (R) and (S) are revealed by the
user, and are shared among trustees. These secrets, which enable owner tracing (but not coin
20   tracing), are thus vulnerable to attack during the token withdrawal protocol. Hence the entity
handling the user secrets acts essentially like a trusted dealer. This may be acceptable if sufficient
controls on handling of user secrets are set in place.

Another possibility is to make the bank effectively act as a trustee. The user's identifier
ID_U could be identical with respect to the bank and the trustee. It is possible, however, for the
25   user to identify herself as ID_U with respect to the bank and separately as ID_U' with respect to the
trustee, where ID_U' is a pseudonym authorized and recorded by the bank and mathematically
unrelated to ID_U. In this manner, both the trustee and the bank must participate in tracing. Of
course, the user would need to shield her real-world identity from the trustee during the token
withdrawal protocol. This can be achieved by having the bank serve as a proxy server for the user,

- 17 -

by using an anonymous store-and-forward approach to token distribution, or by having tokens pre-loaded on smart cards that are then distributed by the bank.

The following discussion describes four aspects of the security of our scheme, user anonymity, non-forgeability of coins, traceability, and the inability of the trustee to steal the user's cash. We are able to prove that our system is secure in all four of the above senses, relative to underlying cryptographic primitives. To provide a flavor of the proof techniques employed here, we give a rigorous proof of the security of user anonymity. In other cases, we provide proof sketches.

With regard to user anonymity, the bank should not be able to extract any information from its interactions with users that reveals which coins have been withdrawn by whom. As we shall show, the security of user anonymity in our system is dependent on k_1, the security parameter, i.e., seed length in bits, of the pseudo-random number generator. (In one embodiment, an acceptable level of security is achieved by letting k_1 be about 80.)

In the underlying blind RSA signature scheme, anonymity is unconditional, i.e., information theoretically secure. In particular, use of the blinding factor (r) ensures that the bank receives no information about withdrawals. In our system, however, we introduce a pseudo-random number generator (PS) to enhance efficiency. We prove the security of anonymity relative to that of (PS). As mentioned above, the two random seeds, (R) and (S), can in practice be reduced to one seed (S). In our proofs, we shall assume that this is the case.

First some definitions. Let PS_S denote the output (of an appropriate length) of (PS) given seed (S). Let (A) be a polynomial time algorithm that outputs a 0 or a 1. Let $EX_Z[A(M)]$ denote the expected output of algorithm A given input M over uniform random choices of Z, i.e., the probability that A(M)=1. The pseudo-random generator (PS) may be said to be broken if a polynomial time algorithm (A) may be found such that $|EX_S[A(PS_S)] - EX_R[A(R)]| = 1/poly$.

The idea behind the proof is simple: user anonymity is information theoretically secure in the case where the user employs purely random inputs. If user anonymity can be broken in the case where the user employs a pseudo-random number generator, then it is possible to distinguish between random and pseudo-random inputs. This is equivalent to breaking the pseudo-random number generator. In other words, if the bank is able to break the anonymity in this scheme, then it can break the pseudo-random generator (PS).

- 18 -

This is true because the values $\{M_i = MAC_w(r_i^3 f(x_i))\}$ are generated using the values (w) and $r_i^3 f(x_i)$ as inputs. These $\{M_i\}$ thus can only provide the bank with information about values it already sees in the clear. These $\{M_i\}$ provide no information that might enable the bank to break user anonymity.

5   Let (D) be an algorithm constructed as follows. Algorithm (D) takes as input three bitstrings, (X), (Y), and (Z), as well as a polynomial time algorithm (B). Algorithm (D) simulates a user 1 using bitstring (X) as a source of randomness and simulates a user 2 using bitstring (Y) as a source of randomness. The bitstring (Z) serves as a source of randomness for algorithm (B). Algorithm (B) simulates the bank in the anonymous withdrawal scheme and then attempts to
10   break the anonymity of the scheme. It does this relative to withdrawals conducted by simulated users user 1 and user 2 in accordance with the experiment described in the definition of blindness above. If the algorithm (B) guesses successfully in this experiment, then (D) outputs a 1 and we write $D_B(X,Y,Z)=1$. Otherwise $D_B(X,Y,Z)=0$, i.e., (D) outputs a 0. The algorithm (D) may be viewed as a distinguishing algorithm: it tries to use (B) to distinguish between the distributions
15   from which (X) and (Y) are drawn.

It is clear from the definition of blindness in above that the anonymity of our scheme is insecure if there exists an algorithm (B) such that $EX_{S,S',Z}[D_B(PS_S, PS'_S, Z)] = 1/2 + 1/poly$. In order words, the anonymity of our scheme is insecure if it is possible to distinguish between the withdrawals of a user 1 with secret seed (S) and a user 2 with secret seed S'. Recall that the
20   underlying anonymous withdrawal scheme is information theoretically secure. Thus for all algorithms (B), it is trivially the case that $EX_{R,R',Z}[D_B(R,R',Z)] = 1/2$, i.e. there is no way to distinguish between two truly random sources. It is easy to see therefore that if there is some polynomial time algorithm (B) such that $EX_{S,R,Z}[D_B(R, PS_S, Z)] = 1/2 + 1/poly$, then (PS) is insecure. We will now show how a compromise of anonymity leads to this situation.

25   Suppose our scheme is insecure and thus there exists an algorithm (B) such that $EX_{S,S',Z}[D_B(PS_S, PS_{S'}, Z)] = 1/2 + 1/poly$. We can then construct a polynomial time algorithm D'(X) which takes as input a bitstring (X), generates a random seed S', and then outputs $D_B(X, PS_{S'}, Z)$. If (PS) is secure, then $EX_{R,S',Z}[D_B(R, PS_{S'}, Z)] < 1/2 + 1/poly$, so that $EX_R[D'(R)] < 1/2 + 1/poly$. But if $EX_R[D'(R)] < 1/2 + 1/poly$, then $EX_R[D'(R)] - EX_S[D'(PS_S)] = 1/poly$, and thus
30   (PS) is insecure. From this contradiction, it follows that if user anonymity in our scheme is insecure, then (PS) is insecure.

- 19 -

We now proceed to treat the issue of forgeability of coins. The users of the system and the trustee, even in collaboration, should not be able to mint coins without express participation of the bank. The hardness of forgery in our system is determined by security parameter k_2, equal to the length of the modulus (N). (In one embodiment, the security parameter k_2 may safely be set

5   at 1024.)

The secret key (w) shared by the trustee and bank is independent of the secret minting key of the bank. Thus, even if the trustee and user collaborate, they can obtain no more information about the bank's minting key than the user herself could. We thus can show that it is as hard in this scheme for the user and trustee to forge coins collaboratively as it is for the user to do so

10   herself in the underlying blind digital signature scheme. Formal proof of this theorem depends upon the fact that the user can simulate the establishment of a secret key between trustee and bank. In carrying out the withdrawal protocol in the underlying scheme, the user can then simulate both the role of the trustee and the role of the bank in processing trustee tokens. Thus, in our scheme, the trustee can provide no additional information useful to the user in committing

15   forgery.

The theory regards the assurance of the trustee that the user cannot cheat and evade tracing of her coins. The trustee should be able to perform both coin tracing and owner tracing with high probability. The security of tracing in our system is determined by security parameter k_3, equal to the length of the trustee tokens in bits, and by security parameter k_2. (For most purposes,

20   it would be acceptable to let k_3 be 10-50 bits.) We can show that the user must either forge a MAC or forge a coin to cheat successfully in this way. In other words, suppose that the user is able to produce a coin which cannot be traced by the trustee. Then the user was successful at either forging a coin or forging a MAC. This can be shown as follows: If the user is able to produce an untraceable coin (C), then either the user forged (C), or the user withdrew (C) from

25   the bank. If the user withdrew (C), and (C) is untraceable, then the user must have provided the bank with an invalid MAC.

More specifically, it is presumed that the user cannot forge a coin in polynomial time with more than a negligible probability. Therefore the probability that a given coin (C) held by a cheating user is untraceable is roughly equal to the user's ability to forge a MAC. Under

30   reasonable assumptions this is about 2^{k_3}, where k_3 is the length of the trustee tokens in our scheme. Thus, a 10-bit trustee token should yield a probability of less than 1/1000 of the user

- 20 -

being able to evade tracing for a given coin. For most law-enforcement purposes, this should be adequate, particularly as law enforcement officers are likely to have multiple coins available for tracing in most scenarios. Moreover, the user can only verify the correctness of a MAC by interacting with the bank. Her efforts at cheating are thus likely to be detected by the bank before

5   she obtains an untraceable coin. For very high security applications, it may be desirable, however, to use MACs of up to, say, 50 bits. (Note that while MACs of 32 or even 64 bits are typical in most financial transactions, the risks in such cases are much greater, involving the potential for many millions of dollars to be misdirected.)

Finally, we consider the ability of the trustee to steal the user's money. Although the

10   trustee should be able to link the user to her coins, he should not be able to steal her coins or make withdrawals from her account. It is common practice not to consider efforts by the bank to steal the user's money: it is assumed that the bank, which has control of the user's account in any case, must be trusted in this respect.

Although the trustee has access to the secrets of the user employed to generate coin data,

15   the trustee does not have access to the user secret s_U. Therefore, the trustee cannot impersonate the user and withdraw money from the user's account without the bank's collusion. This yields the following theorem: it is infeasible for the trustee to steal money from the user's account without the collusion of the bank or the user. This can be shown as follows: The bank only withdraws money from the user's account if authorized to do so through a channel authenticated by means of

20   the user's secret s_U. This channel is authenticated so that no eavesdropper, even the trustee, can steal the user's coins.

In our exposition above, we assume the trustworthiness of trustee, and that the MAC held jointly by the trustee and bank is well protected. In some scenarios, it may be desirable to make weaker security assumptions. We can achieve this --at the cost of computational and storage

25   efficiency-with more extensive record keeping and use of digital signatures by the trustee.

If an attacker manages to seize the MAC shared by the bank and the trustee, and the theft goes undetected, he can present false trustee authorization to the bank. This would enable him to withdraw untraceable coins. There are many possible defenses against this attack, representing a spectrum of tradeoffs between efficiency and security. One possible countermeasure would be to

30   refresh the shared MAC on a frequent basis. If this MAC is generated collaboratively between the

- 21 -

bank and trustee, then forward secrecy may be obtained with respect to either one of the two parties. Thus, if an attacker were to seize the current MAC undetected, he would have only a narrow window of time in which to exploit it. Another option would be to have the trustee digitally sign tokens using a public key signature algorithm, rather than MACing them. The

5   signing key of the trustee could then be distributed among multiple entities using distributed sharing and signature techniques. While this variant on our scheme provides stronger security guarantees, is rather less efficient in terms of the computation required to produce a token.

In the above variants, if a coin (C) is presented to the trustee and the coin cannot be traced, it is unclear whether the trustee or the bank permitted withdrawal of an untraceable coin.

10   This can be remedied by having the trustee digitally sign all tokens, and requiring the bank to keep track of all coin withdrawal transcripts for each user and the trustee to keep track of the number of token withdrawals. If untraceable coins surface, then the bank and trustee records can be compared, and a determination made as to whether the cheating party is the bank or the trustee.

As described above, the trustee can frame the user. In particular, the trustee can generate

15   a value (X) based on a pair of values (r_i, s_i) not yet employed by the user (or based on false seed pair (R', S'), withdraw from the bank a coin C_i based on x_i, spend the coin on some illicit purchase, and then claim that the user was responsible, adducing the registered seed pair (R,S) as evidence.

It is possible to prevent attacks of this nature as follows. We have the user digitally sign (R,S). We then have the bank record all blinded values presented for signing, as well as the

20   number of withdrawals by the user. The bank rejects any withdrawal request based on a previously presented blinded value. Now if trustee attempts, under a false identity, to withdraw a coin C_i (based on a user's seed pair (R,S) when C_i has already been withdrawn, he will be stopped. If he withdraws a coin C_i not already withdrawn by the user, then the user is able to prove, on revealing (R,S) and adducing the bank's counter as evidence, that she was not responsible for the

25   initial withdrawal of C_i. Hence, framing of the user would require collusion between both the bank and the trustee framing of the user by the bank is infeasible because the bank has no knowledge of (S).

Variations, modifications, and other implementations of what is described herein will occur to those of ordinary skill in the art without departing from the spirit and the scope of the

invention as claimed. Accordingly, the invention is to be defined not by the preceding illustrative description but instead by the spirit and scope of the following claims.

What is claimed is:

- 23 -

Claims

1   1.   A method for obtaining a trustee token from a trustee, comprising the steps of:

2   transmitting to a trustee information describing a blinded digital coin; and

3   receiving from the trustee a trustee token comprising a signature by the trustee on the

4   blinded digital coin.

1   2.   The method of claim 1 wherein the information describing the blinded digital coin

2   is the blinded digital coin.

1   3.   The method of claim 1 wherein the information describing the blinded digital coin

2   comprises a random seed for generating at least one blinded digital coins.

1   4.   The method of claim 3 wherein the information describing the blinded digital coin

2   further comprises a quantity of desired coins for generating at least one blinded digital coins.

1   5.   The method of claim 1, further comprising:

2   before the transmitting step, establishing identity with the trustee using a secret.

1   6.   The method of claim 5 wherein the secret comprises the private key belonging to a

2   public/private key pair.

1   7.   The method of claim 1 wherein the method receiving step comprises receiving

2   from the trustee a trustee token comprising a signature by the trustee on a plurality of blinded

3   coins.

1   8.   A system for obtaining a trustee token from a trustee, comprising:

2   a transmitter transmitting to a trustee information describing a blinded digital coin; and

3   a receiver receiving from the trustee a trustee token comprising a signature by the trustee

4   on the blinded coin.

1   9.   A method for generating a trustee token comprising the steps of:

2   receiving from a user information describing a blinded digital coin;

3   storing the information describing the blinded digital coin and a user identifier; and

4   generating a trustee token using the information describing the blinded digital coin, said

5   trustee token comprising a signature by a trustee on the blinded coin.

1   10.   The method of claim 9 wherein the information describing the blinded digital coin

2   is the blinded digital coin.

- 24 -

1   11.   The method of claim 9 wherein the information describing the blinded digital coin

2 comprises a random seed.

1   12.   The method of claim 9 wherein the information describing the blinded digital coin

2 further comprises a number of desired coins.

1   13.   The method of claim 9 wherein the generating step comprises generating a trustee

2 token using the information describing the blinded digital coin, said trustee token comprising a

3 signature by a trustee on at least one blinded coins.

1   14.   The method of claim 9, further comprising:

2 after the generating step, transmitting the trustee token to the user.

1   15.   The method of claim 9, further comprising:

2 before the receiving step, verifying identity of the user using a secret.

1   16.   The method of claim 9 wherein the generating step comprises:

2 generating a trustee token by using the information describing the blinded digital

3 coin to generate the blinded digital coin; and

4 signing the blinded digital coin.

1   17.   The method of claim 16 wherein the signing step comprises signing the blinded

2 digital coin using a private key of a public/private key pair.

1   18.   The method of claim 16 wherein the signing step comprises signing the blinded

2 digital coin using a MAC (Message Authentication Code).

1   19.   A system for generating a trustee token, comprising:

2 a receiver for receiving from a verified user information describing a blinded digital coin;

3 a data store for storing the information describing the blinded digital coin and a verified

4 user identifier; and

5 a token generator for generating a trustee token using the information describing the

6 blinded digital coin, said trustee token comprising a signature by a trustee on the blinded coin.

1   20.   A method for issuing digital cash, comprising the steps of:

2 receiving a blinded coin and a trustee token from a verified user, said trustee token

3 comprising a signature by a trustee on a blinded coin;

4 verifying the trustee token;

5   deducting an amount from an account associated with the user; and

6   issuing the blinded coin with a value related to the amount deducted from the user's

7   account.

1   21.   The method of claim 20, further comprising:

2   before the receiving step, verifying identity of the user using a secret.

1   22.   The method of claim 20 wherein the verifying step comprises calculating a MAC

2   on the blinded coin.

1   23.   The method of claim 20 wherein the verifying step comprises verifying using a

2   trustee's public key.

1   24.   The method of claim 20 wherein the issuing step comprises signing the blinded

2   coin.

1   25.   A system for issuing digital cash, comprising:

2   a receiver for receiving a blinded coin and a trustee token from a verified user, said trustee

3   token comprising a signature by a trustee on a blinded coin;

4   a verifier for verifying the trustee token;

5   a withdrawal mechanism for deducting an amount from an account associated with the

6   user; and

7   an issuer for issuing the blinded coin with a value related to the amount deducted from the

8   user's account.

1   26.   A method for receiving digital cash from a coin issuer using a trustee token,

2   comprising the steps of:

3   transmitting a blinded digital coin and a trustee token to a coin issuer, said trustee token

4   comprising a signature by a trustee on the blinded coin; and

5   receiving a signature on the blinded digital coin from the coin issuer.

1   27.   A system for receiving digital cash from a coin issuer using a trustee token,

2   comprising:

3   a transmitter transmitting a blinded digital coin and a trustee token to a coin issuer, said

4   trustee token comprising a signature by a trustee on the blinded coin; and

5   a receiver receiving a signature on the blinded digital coin from the coin issuer.

1   28.   A method for obtaining revocably anonymous digital cash from a bank by using a

2   trustee, comprising the steps of:

3   establishing identity with the trustee using a secret;

4   transmitting to the trustee information describing a blinded digital coin;

5   receiving from the trustee a trustee token comprising a signature by the trustee on the

6   blinded coin;

7   transmitting the blinded coin and the trustee token to a bank; and

8   receiving a signature from the bank certifying the blinded coin.

1   29.   The method of claim 28 further comprising the step of:

2   unblinding the coin; and

3   transmitting the coin to a merchant.

1   30.   A method for tracing a digital coin, comprising the steps of:

2   decrypting the coin to reveal a user identifier;

3   matching the user identifier encrypted in the coin to an entity.

1   31.   A method for identifying a digital coin associated with a user, comprising the steps

2   of:

3   matching the user to a user identifier;

4   matching the user identifier to coins transmitted to a trustee; and

5   identifying the coins matched to the user identifier as coins associated with the user.
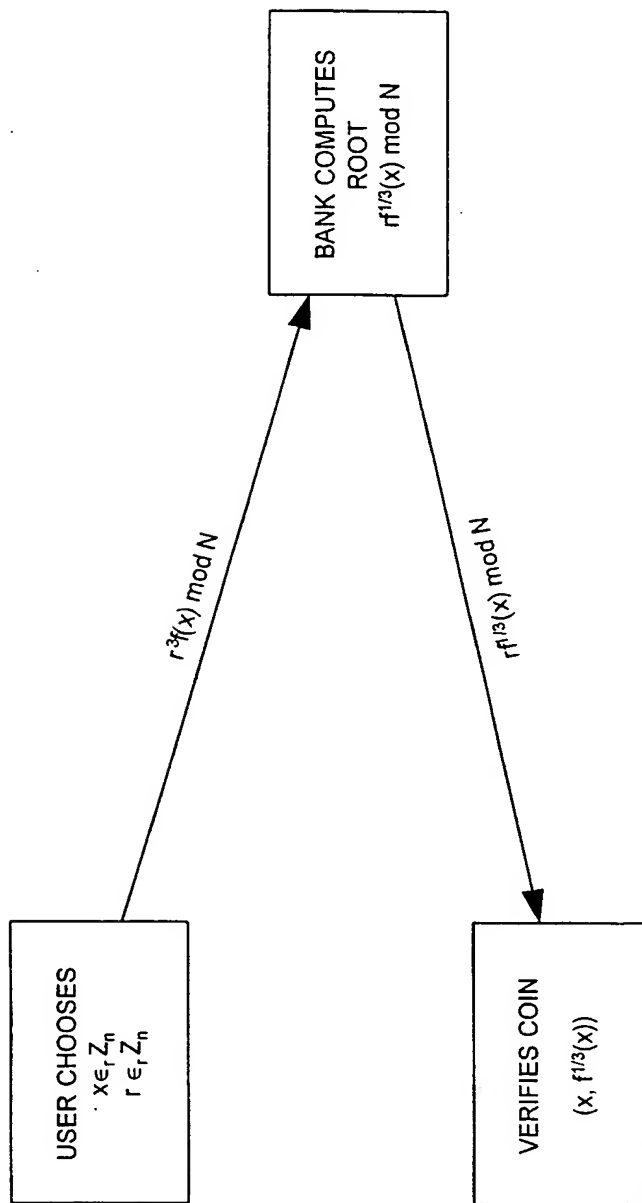
1   32.   A trustee token comprising a signature by a trustee on a blinded coin.

1   33.   The trustee token of claim 32 further comprising a signature by a trustee on a

2   quantity of blinded coins.

1/5

BANK

USER

USER CHOOSES
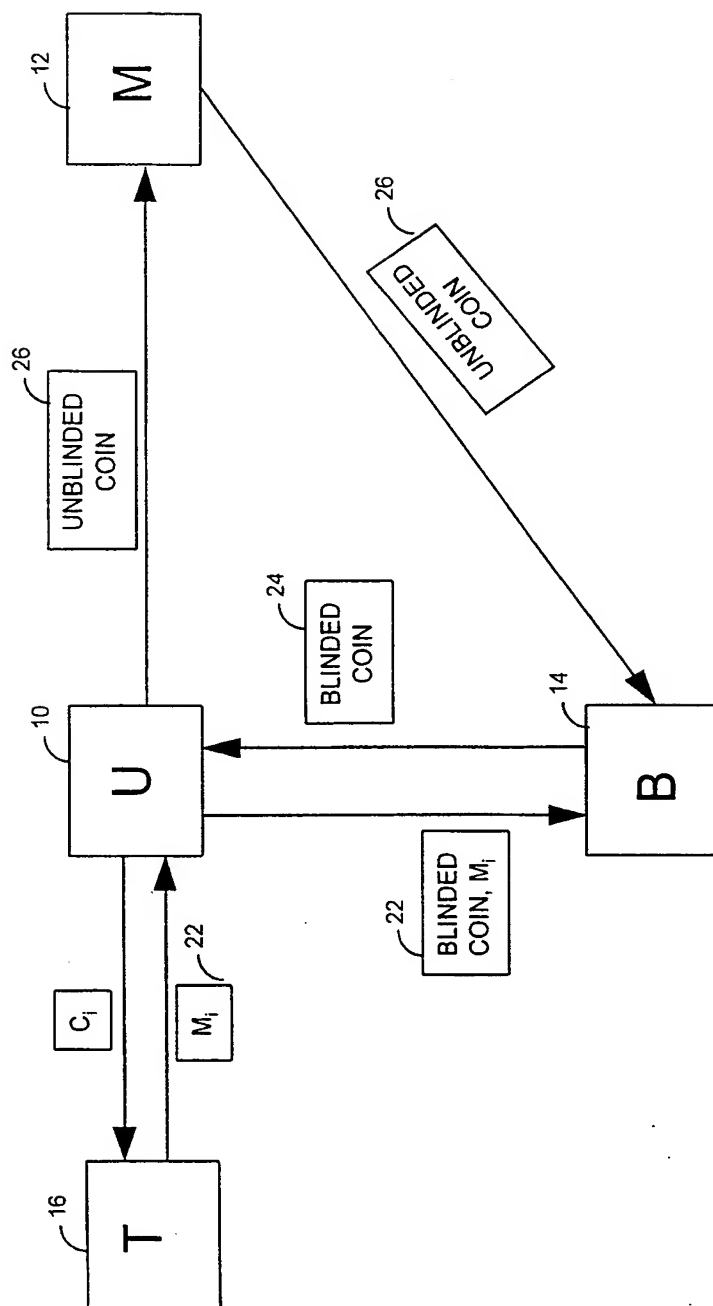$x \in_r Z_n$
$r \in_r Z_n$

$r^3 f(x) \bmod N$

BANK COMPUTES
ROOT
$rf^{1/3}(x) \bmod N$

$rf^{1/3}(x) \bmod N$

VERIFIES COIN
$(x, f^{1/3}(x))$

FIG. 1
PRIOR ART

2/5

FIG. 2

FIG. 3

FIG. 4

5/5

BANK

STEP 152

USER ESTABLISHES
IDENTITY ID_U'
WITH BANK

STEP 162

VERIFIES
$M_i = MAC_w(r_i^{3f}(x_i))$

STEP 164

CALCULATES
$r_i f^{1/3}(x_i)$

154

s_U'

160

$(r_i^{3f}(x_i), M_i)$

166

$r_i f^{1/3}(x_i)$

USER

STEP 150

USER ESTABLISHES
IDENTITY ID_U' WITH
BANK

STEP 156

GENERATE (x_i, r_i)
(IF NECESSARY)

STEP 158

TRANSMIT COIN
AND
TRUSTEE TOKEN

STEP 168

VERIFY
CORRECTNESS OF
COIN
$(x_i, f^{1/3}(x_i))$

FIG. 5

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6   G07F19/00   H04L9/32   G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6   G07F   H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 772 165 A (NIPPON TELEGRAPH & TELEPHONE) 7 May 1997	1,3,5, 7-9,11, 13,15, 17,19, 20, 23-28, 30-33
A	see abstract; claims 1-19; figures 1,6-8,10-15	2,4,6, 10,12, 14,16, 18,21, 22,29
	see column 4, line 54 - column 5, line 16 see column 11, line 12 - column 17, line 31 see column 20, line 12 - column 21, line 59 see column 28, line 41 - column 30, line 3	

-/--

[X] Further documents are listed in the continuation of box C.   [X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 May 1999	12/05/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Guivol, O

4

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	CAMENISCH J ET AL: "FAIR ANONYME ZAHLUNGSSYSTEME" INFORMATIK AKTUELL,18 September 1995, pages 254-265, XP002068945 see the whole document ---	1-3,5, 7-10,13, 15, 19-21, 23-33
X	EP 0 755 136 A (NIPPON TELEGRAPH & TELEPHONE) 22 January 1997 see page 5, line 22 - page 15, line 35 see page 18, line 38 - page 19, line 44; claims 1-5; figures 1,2,5-7,16-19 ---	1,3,5, 7-9,11, 13,15, 17,19, 20, 23-28, 30-33
A	WO 95 22215 A (CHAUM DAVID) 17 August 1995 see the whole document ---	1-33
A	US 5 511 121 A (YACOBI YACOV) 23 April 1996 see the whole document -----	1,8,9, 19,20, 25-33

4

INTERNATIONAL SEARCH REPORT

Information on patent family members

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0772165	A	07-05-1997	JP	9128465 A	16-05-1997
			JP	9244531 A	19-09-1997
			JP	9251499 A	22-09-1997
EP 0755136	A	22-01-1997	JP	9153103 A	10-06-1997
			US	5889862 A	30-03-1999
WO 9522215	A	17-08-1995	US	5712913 A	27-01-1998
			AU	1744895 A	29-08-1995
			EP	0744106 A	27-11-1996
			US	5781631 A	14-07-1998
			US	5878140 A	02-03-1999
US 5511121	A	23-04-1996	CA	2182173 A	31-08-1995
			EP	0746923 A	11-12-1996
			JP	9505169 T	20-05-1997
			WO	9523465 A	31-08-1995